RSAC 2025 Conference

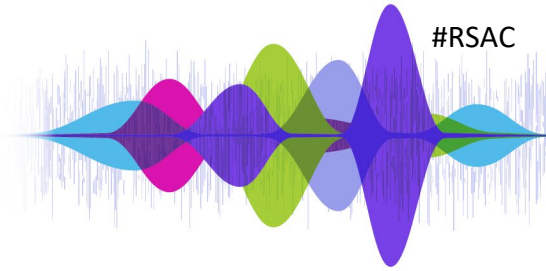
Many Voices.
One Community.

SESSION ID: IDY-R06

Generative AI Meets Identity Governance- Automating the Overlooked

Angelica Faber
Sr. Security Architect
Microsoft
https://www.linkedin.com/in/angelica-faber/

Wesley (Wes) Kuzma
Architect Manager
Microsoft
https://www.linkedin.com/in/wkuzma/

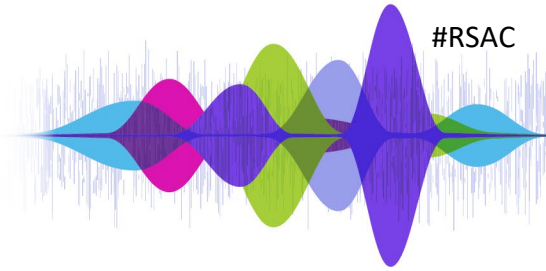


Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.



Agenda

- Why Should I Care About Identity Governance?
- Top 10 Signs You Have Poor Identity Governance
- How can GenAI help?
- Demos
- Apply

Why Should I Care About Identity Governance?

Microsoft alone tracked over 600 million identity attacks during 2024*, these attacks takes advantage of poor identity practices.

- **Overprivileged accounts** expand an attack's blast radius.
- **Dormant accounts** act as hidden backdoors for attackers.
- **Ransomware thrives** on poor role governance, where standard users have unnecessary admin rights.

*Digital Defense Report 2024

TOP 10
SIGNS POOR
IDENTITY
GOVERNANCE
TOP 10

Signs You Have Poor Identity Governance No. 10

The Role Roulette Player

- "Let's just give them some permissions and see what happens!"
- Every access review feels like spinning a roulette wheel—who gets access to what? No one knows!

Signs You Have Poor Identity Governance No. 9

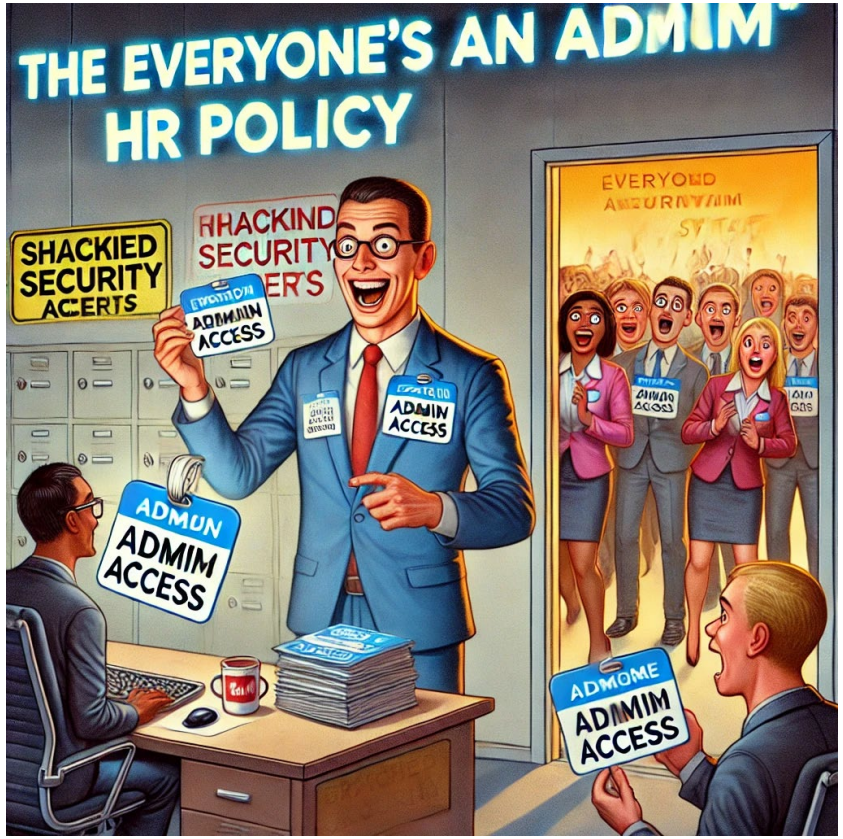
The Copy-Paste Commander

THE COPY-PASTE COMMANDER
JUST COPY THIS ACCESS!
JUST COPY BOB BOD'S ACCESS!
JUST COPY AIR ACCESS!
JUST COPY THIS ACCESS!
GRANT ALL
JUST COPY BOB'S ACCESS! GRAN ALL!

- "Just copy the permissions from Bob."
- Never mind that Bob has been here for a decade and has access to half the company's systems.

Signs You Have Poor Identity Governance No. 8

The "Everyone's an Admin" HR Policy



- Someone just decided to give all new hires blanket admin rights.
- What could possibly go wrong?

Signs You Have Poor Identity Governance No. 7

The Phantom Admin

- No one knows who this is, but there's an admin account floating around with full control, created years ago for a "temporary fix" and forgotten.
- The IT team whispers about it like a campfire horror story.

Signs You Have Poor Identity Governance No. 6

The “But It’s for a Good Cause” Guy

- They know they're breaking access rules, but “It’s just temporary” or “I needed to get work done!”

Signs You Have Poor Identity Governance No. 5

The Overly Generous Approver

- This person treats access requests like a holiday gift exchange – aka. Oprah style.

Signs You Have Poor Identity Governance No. 4

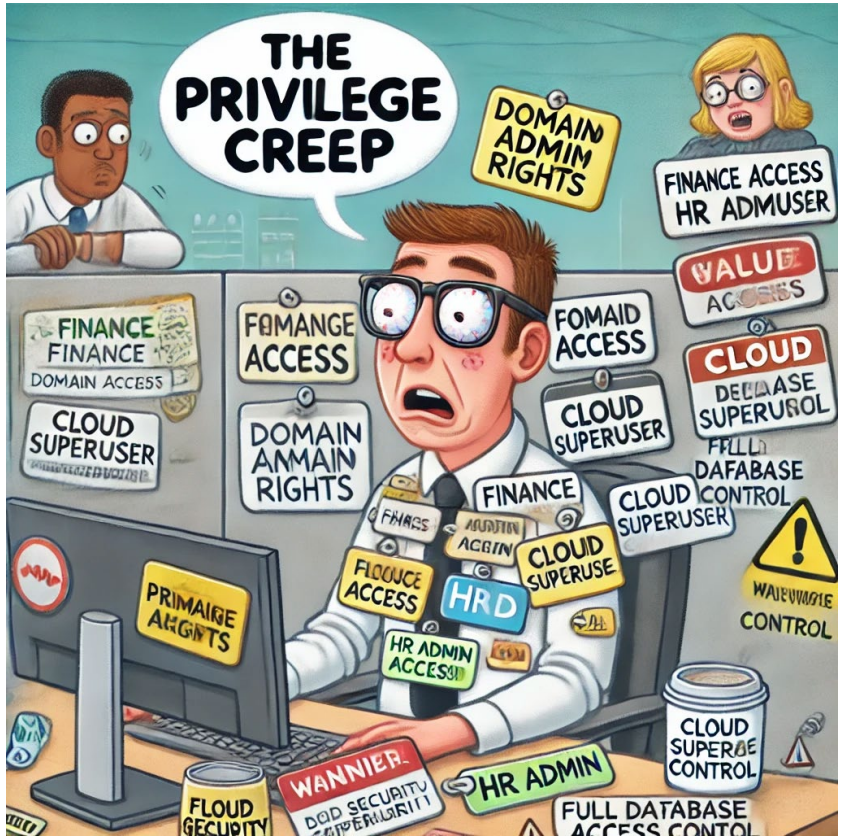
The Shadow IT Sorcerer

- This employee doesn't trust IT processes, so they spin up their own apps, create unauthorized accounts, and grant wide-open access to anyone who asks.

- "What do you mean 'security risk'? It's just a Google Drive link with payroll data!"

Signs You Have Poor Identity Governance No. 3

The Privilege Creep



- The person who slowly, stealthily accumulates permissions over time, not because they asked, but because "it was easier than figuring out who actually needed it."

- One day, they realize they have Domain Admin rights and think, "Oh, cool!"

Signs You Have Poor Identity Governance No. 2

The Ghost in the Company

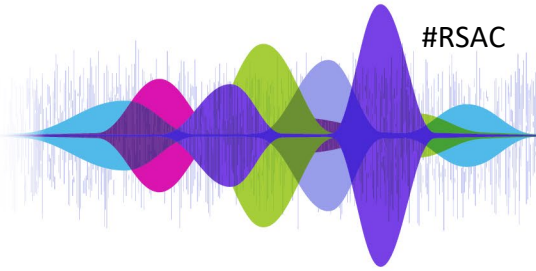
- Former employees whose accounts never get deactivated.
- They haunt the system, lingering with full access to sensitive data, sometimes even years after leaving.
- Bonus points if they still pop up in meetings.

Signs You Have Poor Identity Governance No. 1

The Permissions Hoarder

- That employee who's been around since the dawn of Active Directory.
- Every role change, they just keep accumulating permissions like a digital dragon guarding its treasure.
- "Why remove access? I might need it… someday!"

Existing Identity Governance (IGA) solutions



EVIDEN

Omada

SailPoint

ONE IDENTITY by Quest

Delinea

imprivata®

opentext™

empowerID

IBM

netwrix

PingIdentity

soffid

FISCHER IDENTITY

ORACLE

Saviynt

zilla SECURITY A CyberArk Company

ManageEngine

RSA®

OpenIAM

Tuebora AGENT DRIVEN IGA®

Microsoft Entra IGA

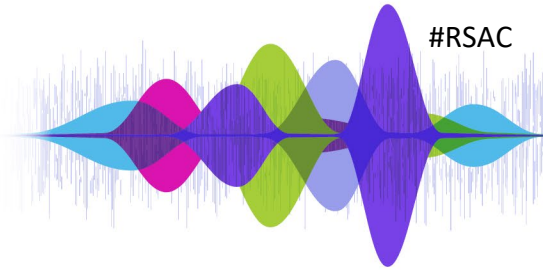
How can GenAI help?

Top 10 Failures	Existing IGA+ solutions	Gen AI can help	Impact
Permissions Hoarder	Access Reviews	Analyze trends, identify movers, and remove access	🔥🔥🔥
Company Ghost	Lifecycle Workflows	Detect orphaned accounts from detached apps	🔥🔥
Privilege Creep	Access Reviews + Access Packages	Proactively detect and remove privileges	🔥🔥
Shadow IT Sorcerer	App Discovery (Private Access)*	Correlate logins & external system activity	🔥🔥
Generous Approver	Access Reviews	Flag suspicious approvals	🔥🔥🔥

How can GenAI help?

Top 10 Failures	Existing IGA+ solutions	Gen AI can help	Impact
Good Cause Guy	Privileged Identity Mgmt + Access Reviews	Analyze approvals and activations, suggest removals + policy changes	
Phantom Admin	Privileged Identity Mgmt + Access Reviews	Correlate activation history with job roles	
Everyone Admin	Privileged Identity Mgmt + Access Reviews	Analyze activation trends and suggest changes	
Copy-Paste Cmdr	Suggested Access Packages	Detect patterns and suggest new Access Pkgs	
Role Roulette Player	Access Packages	Detect patterns and suggest policy changes	

Why GenAI Must Help Fix IGA



Even top-rated IGA platforms struggle because of:

- **Role Complexity:** Role mining is rigid, non-intuitive, and coarse-grained.
- **Static Policies:** Can't adapt to org changes, projects, or usage patterns.
- **Manual Reviews:** Fatigue, rubber-stamping, no context.
- **Lifecycle Gaps:** Movers/joiners/leavers processes often break.
- **Data Issues:** Incomplete metadata, unclear permissions, inconsistent feeds.

GenAI bridges the gap with dynamic reasoning and context:

Existing IGA+ solutions	GenAI-Enhanced
Static role suggestions	Contextual, explainable role generation
Blind access reviews	Usage-based, peer-aware, smart summaries
Rigid workflows	Adaptive, human-in-the-loop recommendations
Manual investigation	Conversational interface for insight
Data silos	Intelligent correlation and enrichment

Demos Description (WIP)

- Automated mover detection and lifecycle management recommendations.
- Monitoring of privileged role usage combined with additional data, such as job roles, to suggest and request role removals.
- Suggest removals of approvers based on approval patterns and additional data, such usage and job roles.
- Suggest new access packages based on various patterns.

RSAC 2025 Conference

Demos

Apply: What Should You Do Next?

- Next Week, You Should:
  - Meet with your IGA and Security teams to discuss Identity Governance risks.
- Within Three Months, You Should:
  - **Map your identity governance** tools and processes.
  - **Use GenAI** to detect excessive permissions and weak approvals.
- Within Six Months, You Should:
  - **Implement continuous identity monitoring** with GenAI-driven governance.
  - **Make identity governance a core security priority** to prevent attacks before they happen.

RSAC™ 2025 Conference

Many Voices.
One Community.